Research, Development, Test & Evaluation (RDT&E)
Security Education Matrix

Click on the appropriate population category below:

Security Personnel	Includes: information security/classification management, computer/information systems security, physical security/access control, special protective officers, security administrators, and other specialized security personnel according to local requirements.
Program Managers	
Scientists and Engineers	
Computer Scientists	Includes: programmers, support staff (network operators, etc.), and ADP operators.
Special Access Program Personnel	
Non-technical Professionals	Includes: logisticians, program analysts, and technical writers.
Technicians	Includes: testers, test/range operators, lower level experimenters, and fabricators. (Personnel in this category are typically non-degreed professionals who assist scientists and engineers).
Counterintelligence and Intelligence Personnel	
Professional Support Staff	Includes: contracting officers, business managers, and controllers.
Administrative Support Staff	Includes: audio/visual and documentary personnel
Support Personnel	Includes: cafeteria, custodial, repair, and transportation personnel.
Co-ops, Interns/Students and University Faculty	
Foreign Nationals	Includes: foreign nationals who work within a facility, foreign liaison officer/international program personnel, and exchange personnel.

Security Personnel Go Back

Security Roles and Responsibilities:

- Overall laboratory security
- Technology Transfer/safeguarding of sensitive information
- Safeguarding and securing of scientific and technical information.
- Security/Counterintelligence roles and responsibilities
- Acquisition Security
- Public Release
- Media and Public Affairs
- Security Education

Security Training Requirements:

- In-depth training on lab security
- Need to provide better integrated support
- Need to understand Acquisition process and milestones
- Need to understand the requirements for the protection of export controlled information and material
- Technology protection

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **DoD Security Specialist** (3 wk course for security specialists) covers security program management issues including information and computer security, physical security, industrial and personnel security, and communications and operations security.
- **Information Security Management** (2 wk course for security professionals) includes comprehensive survey of DoD INFOSEC program policies and procedures.
- **Classification Management** (3 day course for security professionals) covering classification process and related requirements.
- **Special Access Program Orientation** (3 day seminar tailored to host organization requirements) gives tailored on-site training to personnel working with DoD special access programs. Includes orientation to the defense acquisition process, annual review process, inspections and audits, intelligence threats and more.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - Computer Network Defense (CND)
  - Designated Approving Authority (DAA) Basics
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Information Age Technology
  - Information Assurance in Defense in Depth
  - CyberProtect
  - Introduction to the DOD Information Technology Security Certification & Accreditation Process (DITSCAP)
  - Operational Information Systems Security (OISS)
  - Public Key Infrastructure (PKI)
- There are numerous video products available

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/
Relevant courses include:

- **DoD Scientific and Technical Information (STINFO) Program Manager** - (3 day course) provides an understanding of how to carry out the responsibilities of the DoD Scientific and Technical Information Program (STIP). Key topics covered are: control and marking technical information, domestic technology transfer program, DOD STIP programs and offices, DTIC overview, literature searching, STINFO manager duties, and technical publications program.
- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.
- **Introduction to the DOD Scientific and Technical Information Program (STIP)** (Web-based distance learning course)

Defense Institute of Security Assistance Management (DISAM)
http://disam.osd.mil Offers classroom courses such as:

- **International Programs Security Requirements (Short Course)** (2 day course for personnel who are involved in international programs but who do not require the depth of instruction presented in the IPSR Long Course) covers the same programs and basic statutes, international agreements, and national and DoD policies that are covered by the IPSR).
- **International Programs Security Requirements Course (Long Course)** (1 wk course for DoD and other government employees and defense contractor personnel who have "hands-on" involvement in international programs) covers basic statutes, international agreements, and national and DoD policies that are the basis for information security and technology control requirements in international programs. Areas covered are negotiating, managing, executing, or otherwise directly participating in international government or commercial programs. Reviewed are Foreign Military Sales, cooperative R&D, commercial sales, license application review, systems

acquisition, foreign contracting, foreign disclosure, international visits and personnel exchanges, program protection, and industrial security.

USDA Graduate School http://grad.usda.gov/ Offers several related courses:

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.
- **Fundamentals of Computer Security** (10 weeks/evenings/$469) covers PCs to mainframe environments; computer crimes, computer security laws, directives, and regulations, program management, threats and vulnerabilities, hackers, viruses, and personnel security requirements are some topics covered.
- **Computer Viruses, Hacking and Intrusion** (3 hrs, $395) provides a basic understanding of the nature of computer viruses and suggested methods and procedures for identifying and dealing with them.
- **Wireless Technology** (3 days, $795) is designed for IA professionals who require a working knowledge of wireless communication technologies and wireless security.
- **Firewalls: Technology** (3 days, $795) is an introduction for IT professionals to learn how to employ firewalls in a multi-protocol networked environment.

NTIS (Dept. of Commerce) http://www.ntis.gov/products/types/publications.asp?loc=4-4-4 CD-ROM, "The Industrial Security Professional's Desktop Resource Guide for Security Awareness Training and Education" works as a companion to the NISPOM providing guidance on implementing a SATE program, sample briefing materials, etc.

Air Force Institute for Advanced Distributed Learning
http://www.maxwell.af.mil/au/afiadl offers CBT course 0Z100, "Classified National Security Information Management" which covers information security management issues, overview of classification management, declassification exemptions, processes and procedures.

Federal Law Enforcement Training Center www.fletc.gov/ssd/ssd_home.htm offers relevant physical security courses such as:

- **Law Enforcement Media Relations Training Program (LEMRTP)** (4.5 days) provides basic tools for dealing with print, radio, and television media in a professional manner.
- **Physical Security Training Program** (10 days) provides an in-depth knowledge of physical security systems and procedures. This includes conceptual security considerations, vulnerability assessments, and familiarization with hardware and software.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov provides an abundant amount of OPSEC training and materials. Examples are:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Practitioners Course (OPSE2380)** (5 days) provides the program basics, in addition, students learn to apply the program to their own organizations and activities.
- **Operations Security Program Manager Course (OPSE2390)** (3 days) provides detailed instruction on program design, planning, decision briefing, and awareness training.
- **Threat Research for OPSEC (OP2330)** (3 days) provides an overview of information resources available to the OPSEC analyst.
- **OPSEC and Web Content Vulnerability (OPSE2350)** (2 days) focuses on web page content rather than technical security. Relates to open source information.
- **Survey Course for the Practitioner (OPSE3400)** (10 days) prepares you to plan, organize, and conduct an OPSEC survey and produce a final report.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hrs) provides basic OPSEC knowledge.

Program Managers Go Back

Security Roles and Responsibilities:

- Overall program protection
- Endorse Security and CI
- Reprimand offenses

Security Training Requirements:

- Security Awareness – high level (in-depth)
- Formal training to identify critical information. Assess and apply protection and safeguards.
- Implement disclosure regimes.
- Need to understand the requirements for the protection of export controlled information and material.
- Technology protection

Additional Comment: Security Awareness should also be included in the general program management courses.

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.
- **Special Access Program Orientation** (2 -4 day seminar tailored to host organization requirements) gives tailored on-site training to personnel working with DoD special access programs. Includes orientation to the defense acquisition process, annual review process, inspections and audits, intelligence threats and more.

Defense Institute of Security Assistance Management (DISAM)
http://disam.osd.mil/ Offers classroom courses such as:

- **International Programs Security Requirements (Short Course)** (2 day course for personnel who are involved in international programs but who do not require the depth of instruction presented in the IPSR Long Course) covers the same programs and basic statutes, international agreements, and national and DoD policies that are covered by the IPSR).

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Information Age Technology
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/ Relevant courses include:

- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Scientists & Engineers Go Back

Security Roles and Responsibilities:

- Developers of RDT&E information

Security Training Requirements:

- Security Awareness—high level (in-depth)
- Formal training in the identification of critical information (classification/protection determinants, releasability, etc.)
- Need to understand the requirements for the protection of export controlled information and material
- Technology protection

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.
- **Special Access Program Orientation** (2 -4 day seminar tailored to host organization requirements) gives tailored on-site training to personnel working with DoD special access programs. Includes orientation to the defense acquisition process, annual review process, inspections and audits, intelligence threats and more.

Defense Institute of Security Assistance Management (DISAM)
http://disam.osd.mil Offers classroom courses such as:

- **International Programs Security Requirements (Short Course)** (2 day course for personnel who are involved in international programs but who do not require the depth of instruction presented in the IPSR Long Course) covers the same programs and basic statutes, international agreements, and national and DoD policies that are covered by the IPSR).

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Information Age Technology

- Public Key Infrastructure (PKI)
- There are numerous video products available

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/
Relevant courses include:

- **DoD Scientific and Technical Information (STINFO) Program Manager** - (3 day course) provides an understanding of how to carry out the responsibilities of the DoD Scientific and Technical Information Program (STIP). Key topics covered are: control and marking technical information, domestic technology transfer program, DOD STIP programs and offices, DTIC overview, literature searching, STINFO manager duties, and technical publications program.
- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.
- **Introduction to the DOD Scientific and Technical Information Program (STIP)** (Web-based distance learning course)

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Computer Scientists Go Back

Security Training Requirements:

- Security Awareness—high level (in-depth)

Existing Training & Awareness Courses/Products

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - Computer Network Defense (CND)
  - Designated Approving Authority (DAA) Basics
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Information Age Technology
  - Information Assurance in Defense in Depth
  - Information Operations (IO) Fundamentals
  - System Administrator Incident Preparation & Response for UNIX
  - Secret and Below Interoperability (SABI)
  - UNIX Security for System Administrators
  - Windows NT Security
  - CyberProtect
  - Information Assurance (IA) for Auditors & Evaluators
  - Introduction to Computer Incident Response Team (CIRT) Management
  - Introduction to the DOD Information Technology Security Certification & Accreditation Process (DITSCAP)
  - Operational Information Systems Security (OISS)
  - Public Key Infrastructure (PKI)
  - System Administrator Incident Preparation & Response (SAIPR) for Windows NT
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/: Offers several related courses:

- **Fundamentals of Computer Security for Federal Information Systems** (5-day course/$595) provides computer security professionals with an overview of security issues specific to the Federal government; covers all areas of training mandated by Computer Security Act of 1987.
- **Data Security and Cryptography** (10 weeks/ evenings) is designed for computer and communication engineers interested in embedded security into an information system, security attacks, access controls, public-key cryptography, classical cryptography, authentication and digital signatures, protocols, and security engineering.

- **Introduction to Cyberwarfare (ISS Certification)** (5 days) teaches overall computer security program management and policy.
- **Introduction to Information Security** (5 days) is an introductory course for students to gain essential skills, concepts, tools and terminology of the field, for IT professionals.
- **Security in IT Applications** (1 day, $395) is designed to provide basic understanding of features and techniques for incorporating computer security into the design and development of software applications.
- **Information Security Specialist Certificate** (10 days,$2500) is a combination of cyperwarfare and information security. This includes hands-on target identification and attack labs to illustrate infiltration techniques.
- **Windows NT Security Course for Systems** (TCOM9945T-W01, 5 days, $1195, system administrator, network managers or IS technical staff) teaches how to design and implement an NT security plan, understand basics of computer system security, log on security, understand C2-level security requirements and more.
- **Unix Security for Systems Administrators** (SRTY9984T-W01, 5 days, $995, system administrators and network security personnel) the define and present UNIX security features, provide standards, describe functional features in security profile tools, provide beneficial use of freeware hacking tools and more.

Information Resource Management College http://www.ndu.edu/irmc/ offers many computer related courses relevant to security, here are a few:

- **Information Assurance Certification Program** (NSTISSI No. 4011, no fee for DOD, non-DOD $850, higher level course with many prerequisites) provides in-depth examination of practical challenges concerning the protection of enterprise information systems.
- **Managing Information Security In a Networked Environment (SEC)** provides "defense in depth" perspective on protecting computer-based information in a modern networked environment
- **Security, Privacy, and Access Issues in eGovernment (SPA)** is where students evaluate eGovernment processes, technical architectures, and organization policies to assess potential security and privacy risks.

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/
Relevant courses include:

- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Special Access Program Personnel Go Back

Security Roles and Responsibilities:

- Must protect SAP information IAW security classification guides, OPSEC guide, etc.

Security Training Requirements:

- Security Awareness—High with special information, as needed

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.
- **Special Access Program Orientation** (2 -4 day seminar tailored to host organization requirements) gives tailored on-site training to personnel working with DoD special access programs. Includes orientation to the defense acquisition process, annual review process, inspections and audits, intelligence threats and more.
- **Information Security Management** (2 weeks, security professionals) offers a more intense course than the Information Security Orientation.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Practitioners Course (OPSE2380)** (5 days) provides the program basics, in addition, students learn to apply the program to their own organizations and activities.
- **Operations Security Program Manager Course (OPSE2390)** (3 days) provides detailed instruction on program design, planning, decision briefing, and awareness training.
- **Threat Research for OPSEC (OP2330)** (3 days) provides an overview of information resources available to the OPSEC analyst.
- **OPSEC and Web Content Vulnerability (OPSE2350)** (2 days) focuses on web page content rather than technical security. Relates to open source information.

- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hrs) provides basic OPSEC knowledge.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - Computer Network Defense (CND)
  - Designated Approving Authority (DAA) Basics
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Information Age Technology
  - Information Assurance in Defense in Depth
  - CyberProtect
  - Introduction to the DOD Information Technology Security Certification & Accreditation Process (DITSCAP)
  - Operational Information Systems Security (OISS)
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/ Offers several related courses:

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Non-technical Professionals Go Back

Security Training Requirements:

- Security Awareness—medium level

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/ Relevant courses include:

- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Technicians Go Back

Security Training Requirements:

- Security Awareness—level depends on the individual's access to classified information and should be mapped against that access—decision to be made locally
- Training may be needed to apply classification or protection, safeguard through the testing process

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Defense Technical Information Center (DTIC) http://www.dtic.mil/dtic/training/ Relevant courses include:

- **Marking Technical Documents Course** - (1 day course) provides an understanding of the rationale and mechanics of properly assigning distribution statements, the For Official Use Only (FOUO) marking, and the export control warning notice to DOD STINFO.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Counterintelligence & Intelligence Personnel Go Back

Security Roles and Responsibilities:

- Overall lab CI support

Security Training Requirements:

- Requirements for CI support to RDT&E facilities

Existing Training & Awareness Courses/Products

Attend specialized CI training for CI support to RDT&E facilities offered at the Joint CI Training Academy

Attend service department CI course

Professional Support Staff Go Back

Security Roles and Responsibilities:

- Have a direct impact on projects and programs. People they hire and/or manage have major impact on programs

Security Training Requirements:

- Security Awareness—level depends on the individual's access to classified information and should be mapped against that access. For example, high if working with SAP or CO. Decision to be made locally.

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.
- **Special Access Program Orientation** (3 day seminar tailored to host organization requirements) gives tailored on-site training to personnel working with DoD special access programs. Includes orientation to the defense acquisition process, annual review process, inspections and audits, intelligence threats and more.

Federal Acquisition Institute http://www.gsa.gov provides classroom and Internet-based training for CORs and others who need to understand Federal contracting and acquisition processes. Example: "Contracting Orientation" course -- introduction to the Federal acquisition process.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Administrative Support Staff Go Back

Security Training Requirements:

- Security Awareness—level depends on the individual's access to classified information and should be mapped against that access—decision to be made locally.

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

USDA Graduate School http://grad.usda.gov/

- **Information Technology Security** (1-day class/$195) explores basic concepts of IT security (confidentiality, integrity, availability and legality); examines relevant laws (Clinger/Cohen Act, Foreign Corrupt Practices Act, Computer Security Act, Computer Fraud and Abuse Act, Privacy Act and FOIA); details ITS threats and vulnerabilities.

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Support Personnel

Security Training Requirements:

- Security Awareness—level depends on the individual's access to classified information and should be mapped against that access—decision to be made locally.

Existing Training & Awareness Courses/Products

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Co-ops, Interns/Students, and University Faculty Go Back

Security Training Requirements:

- Security Awareness—level depends on the individual's access to classified information and should be mapped against that access—decision to be made locally
- This group typically has short-term involvement with high risk. They need formal training if accessed to classified information to include handling, safeguarding, destruction, etc.

Existing Training & Awareness Courses/Products

Defense Security Service (DSS) http://www.dss.mil/training/index.htm Relevant courses include:

- **Information Security Orientation** (2-day basics class for DoD personnel working with classified information, available as resident and televised version) class provides working knowledge of classification, how to downgrade/declassify information, how to safeguard against unauthorized disclosure and discusses marking and security violations.

Defense Information Systems Agency (DISA) http://iase.disa.mil DISA's Information Assurance Education, Training, Awareness, and Products Branch develops, coordinates and supports information assurance training.

- Web based training (WBT) courses include:
  - DOD Information Assurance Awareness
  - Federal Information Systems Security Awareness
  - Public Key Infrastructure (PKI)
- There are numerous video products available

Interagency Operations Security Support Staff (IOSS) www.ioss.gov Relevant courses include:

- **Operations Security Fundamentals (OPSE1300)** (1 day) is designed to provide federal employees and federal contractors the basics of operations security.
- **Operations Security Fundamentals CBT (OPSE1301)** (on-line, 4 hours) provides basic OPSEC knowledge.

Foreign Nationals Go Back

Security Roles and Responsibilities:

- Access restricted to public domain and open source, as appropriate

Security Training Requirements:

- Security Awareness—They need to know what's expected of them. Level of awareness instruction should be mapped against their role in the lab. This will be an unclassified briefing

Existing Training & Awareness Courses/Products

No specific resources identified for this population

Back to Top